The Sydney Morning Herald

Technology Cybersecurity

Players' passports, contracts exposed in Football Australia data leak

David Swan and Vince Rugari

February 1, 2024 — 12.38pm

Listen to this article
5 min

Australian soccer players have had their passports, contracts and other personal information leaked online in a cybersecurity incident that has potentially also affected every local customer or fan, researchers say.

Football Australia leaked secret keys online, giving public access to more than 100 buckets of data including players' personal documents and contracts, according to Cybernews, an independent cybersecurity research publication.

Football Australia, the governing body that controls teams like the Matildas, has exposed players' information, according to an independent cybersecurity research publication. GETTY

The researchers said the leak, which was probably due to human error and not a cyberattack, included players' passport details along with customers' ticket purchase information, and internal infrastructure details.

"While we cannot confirm the total number of the affected individuals, as it would require downloading the entire dataset, contradicting our responsible disclosure policies, we estimate that every customer or fan of Australian football was affected," the Cybernews researchers said. "The exposed data, including contracts and documents of football players, poses a severe threat as attackers could exploit this information for identity theft, fraud, or even blackmail, emphasising the urgent need for improved security practices and measures to safeguard sensitive data."

'Considering the exposure lasted for at least 681 days, it's plausible that external attackers discovered and utilised these keys.'

Jamieson O'Reilly, founder of cybersecurity firm Dvuln

Football Australia had left plain-text Amazon Web Services (AWS) keys exposed online, the researchers said, enabling access to 127 digital storage containers. The organisation fixed the issue after being made aware of it, the researchers said.

FA said it was aware of the possible data leak and was investigating it as a priority. “Football Australia takes the security of all its stakeholders seriously. We will keep our stakeholders updated as we establish more details,” FA said in a statement.

The federation, headquartered in Sydney, is the governing body for Australia’s soccer, futsal and beach soccer teams.

The leak was independently confirmed by cybersecurity researcher Jamieson O’Reilly, founder of cybersecurity firm Dvuln.

“Considering the exposure lasted for at least 681 days, it’s plausible that external attackers discovered and utilised these keys,” he said.

Football Australia CEO James Johnson: The soccer organisation has suffered a mass cybersecurity incident.
JAMES BRICKWOOD

“This data is highly sensitive, particularly the personally identifiable information of players and the infrastructure scripts, which could contain more credentials, leading to further unauthorised access.

“The lack of effective monitoring in this case raises questions about the security practices in place. Regular monitoring for unusual activities or unauthorised access can quickly flag potential security breaches.”

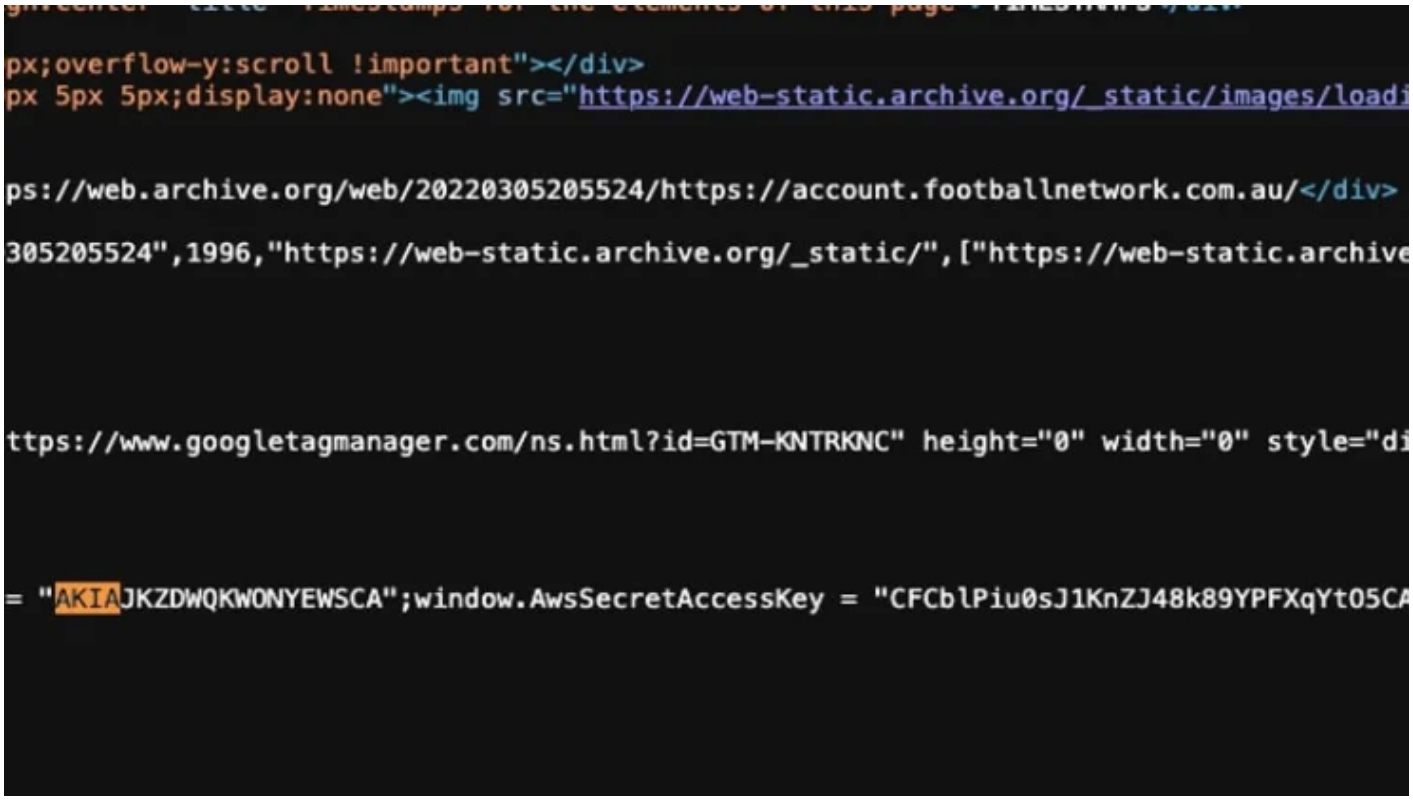
Katherine Mansted, executive director of cyber intelligence at CyberCX, said that the leak highlighted the sensitive and valuable information held by sporting organisations.

“It’s also a reminder that not all data breaches have a malicious actor behind them,” she told this masthead. “As we digitise, the risk of making mistakes grows for all of us, and we need to make sure that our cybersecurity and awareness grow with that risk.

“Even though this was a mistake, the information was accessible online for nearly 700 days, and it’s the type of information that would be highly attractive to opportunistic cyber criminals. And unfortunately it’s impossible to pull that data back.”

The breach is the latest cybersecurity incident to affect a high-profile Australian organisation.

Late last year, researchers discovered a data breach impacting Melbourne travel agency Inspiring Vacations, in which a non-password protected database containing about 112,000 records totalling 26.8 gigabytes was leaked online.



An image showing a secret key that allowed Football Australia data to leak. JAMIESON O’REILLY

Tens of millions of Australians have been caught up in recent security breaches including customers of Optus, HWL Ebsworth, Latitude Financial, Medibank, DP World and Dymocks, in what’s being dubbed a “new normal” of consistent attacks and leaks.

The Optus data breach was similar to the incident affecting Football Australia in that an unprotected endpoint left the personal data of some 10 million customers publicly exposed and subsequently leaked to the dark web.

That breach led to new legislation significantly increasing penalties for serious or repeated breaches of customer data. Organisations that fail to adequately protect peoples’ data face fines of $50 million or more.

“When Australians are asked to hand over their personal data they have a right to expect it will be protected,” Attorney-General Mark Dreyfus said when introducing the legislation.

“Unfortunately, significant privacy breaches in recent weeks have shown existing safeguards are inadequate. It’s not enough for a penalty for a major data breach to be seen as the cost of doing business.”

The Market Recap newsletter is a wrap of the day’s trading. Get it each weekday afternoon.

David Swan is the Technology Editor for The Age and The Sydney Morning Herald. He was previously Technology Editor for The Australian newspaper. Connect via Twitter or email.

Vince Rugari is a sports reporter for The Sydney Morning Herald. Connect via Twitter or email.